UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

PROPUESTA DE UN SISTEMA DE CONTROL INTERNO INFORMÁTICO PARA LOS LABORATORIOS DE COMPUTACIÓN DE LA UACE DE LA UTMACH

RODRIGUEZ YANZA ELBA GIANELLA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2018

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

PROPUESTA DE UN SISTEMA DE CONTROL INTERNO INFORMÁTICO PARA LOS LABORATORIOS DE COMPUTACIÓN DE LA UACE DE LA UTMACH

RODRIGUEZ YANZA ELBA GIANELLA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2018

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

PROPUESTA DE UN SISTEMA DE CONTROL INTERNO INFORMÁTICO PARA LOS LABORATORIOS DE COMPUTACIÓN DE LA UACE DE LA UTMACH

RODRIGUEZ YANZA ELBA GIANELLA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

ORDÓÑEZ BRICEÑO KARLA FERNANDA

MACHALA, 18 DE JULIO DE 2018

MACHALA
18 de julio de 2018

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado PROPUESTA DE UN SISTEMA DE CONTROL INTERNO INFORMÁTICO PARA LOS LABORATORIOS DE COMPUTACIÓN DE LA UACE DE LA UTMACH, hacemos constar que luego de haber revisado el manuscrito del precitado trabajo, consideramos que reúne las condiciones académicas para continuar con la fase de evaluación correspondiente.

ORDÓÑEZ BRICEÑO KARLA FERNANDA
0705031003
TUTOR - ESPECIALISTA 1

CHIMARRO CHIPANTIZA VICTOR LEWIS
0703703413
ESPECIALISTA 2

PARRA OCHOA EUDORO BENITO
0701063406
ESPECIALISTA 3

Fecha de impresión: miércoles 18 de julio de 2018 - 10:02

URKUND

Urkund Analysis Result

Analysed Document: RODRIGUEZ YANZA ELBA GIANELLA_PT-010518.pdf (D40270236)
Submitted: 6/20/2018 4:40:00 AM
Submitted By: titulacion_sv1@utmachala.edu.ec
Significance: 0 %

Sources included in the report:

Instances where selected sources appear:

0

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

La que suscribe, RODRIGUEZ YANZA ELBA GIANELLA, en calidad de autora del siguiente trabajo escrito titulado PROPUESTA DE UN SISTEMA DE CONTROL INTERNO INFORMÁTICO PARA LOS LABORATORIOS DE COMPUTACIÓN DE LA UACE DE LA UTMACH, otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

La autora declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

La autora como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 18 de julio de 2018

RODRIGUEZ YANZA ELBA GIANELLA
0705389013

RESUMEN

La seguridad del ambiente informático, desde todos sus puntos, se ha convertido en una necesidad inherente al proceso administrativo exitoso. La falta de evaluación y actualización de los procesos de control interno ha generado una serie de complicaciones y conflictos, que ha derivado en la inconsistencia, en el menor de los casos, hasta una pérdida irreparable de información crítica, sobre la cual se basan decisiones importantes para el buen funcionamiento de una organización, por lo que se considera de suma importancia la redefinición de procesos de control eficaces y la consiguiente elaboración de políticas para poder alcanzar los objetivos de un ambiente de información eficiente y confiable. Para el desarrollo de la presente investigación, se inició con la recopilación y análisis de los diferentes marcos de trabajo para aplicar una auditoría informática, además se procederá a estudiar y analizar las estrategias y principios de la administración financiera desde el punto de vista informático, que se han utilizado para proteger y resguardar los activos, además de evaluar la planeación, organización y situación actual de los Sistemas de Información de la Universidad Técnica de Machala, enfocándose en las estrategias, tácticas e infraestructura tecnológica de información. Posteriormente se generará la metodología de control interno informático en donde se detallan todos los procesos para que el área informática trabaje de una manera correcta y alineada a las normas de seguridad actuales.

Palabras clave: control, control informático, seguridad informática, controles preventivos, controles correctivos

ABSTRACT

He lack of evaluation and updating of internal control processes has generated a series of complications and conflicts, which has resulted in inconsistency, in the smallest of cases, to an irreparable loss of critical information, on which important decisions are based. for the proper functioning of an organization, which is why it is considered extremely important to redefine effective control processes and the consequent development of policies to achieve the objectives of an efficient and reliable information environment.

For the development of this research, it began with the collection and analysis of the different frameworks for applying computer control, in addition, it will proceed to study and analyze the strategies and principles of financial administration from the computer point of view, which they have been used to protect and safeguard the assets, in addition to evaluating the planning, organization and current situation of UACE laboratories of UTMACH, focusing on strategies, tactics and information technology infrastructure. Subsequently, the internal computer control methodology will be generated where all the processes are detailed so that the computer area works in a correct manner and aligned with the current security standards.

Keywords: control, computer control, computer security, preventive controls, corrective controls

ÍNDICE

INTRODUCCIÓN

En la actualidad, la globalización y el rápido avance de las organizaciones, así como la importancia que se le otorga a la información, el cual es considerado el principal activo, parte fundamental del crecimiento y desarrollo de una organización, han contribuido a cambiar en gran medida la manera en cómo piensan las personas, aunado a la información se encuentran los equipos que dan soporte para el manejo de esta información.

Estableciendo la importancia del uso de mecanismos de control informático aplicables a los laboratorios de informática de la Universidad Técnica de Machala, lo que se analiza es la necesidad de establecer políticas y herramientas que sean necesarias para disponer de elementos suficientes para que los procesos y actividades que llevan a cabo dentro de los laboratorios se realicen con eficiencia y eficacia y que los recursos sean utilizados de manera adecuada, buscando de esta manera aportar al logro y consecución de los objetivos institucionales.

En el laboratorio de informática de la Unidad Académica de Ciencias Empresariales se brinda apoyo a estudiantes y docentes a través del préstamo de equipos de cómputo con acceso a internet y al resto de servicios en línea con los que cuenta la Universidad Técnica de Machala. En este contexto, el uso del laboratorio se ha convertido en una necesidad indispensable del proceso educativo. De esta manera la falta de evaluación y por ende la actualización de los procesos de control puede llegar a generar una serie de problemas y conflictos que afectan el normal desenvolvimiento de las actividades realizadas en dicho lugar, por lo que se considera de gran importancia, establecer procesos de control que resulten eficaces, y la elaboración de políticas para alcanzar los objetivos de un ambiente de trabajo con equipos que resulten adecuados para el trabajo educativo.

Siendo así que para la presente investigación se manifiesta la importancia del control interno informático, entendiéndose como este al sistema integrado al proceso administrativo, que forma parte activa de la planeación, organización, dirección y control de las operaciones

realizadas, que tiene como propósito la protección de los recursos informáticos a través de la mejora en los indicadores de eficiencia y productividad de las actividades.

El propósito principal de la Auditoría Informática es la comprobación de la fiabilidad de los equipos informáticos y el uso que se hace de la información, además contribuye con medios de seguimiento y propone la aplicación de nuevas estructuras o en su defecto de nuevos métodos que se apliquen a la actividad, que en este caso será el manejo de información automatizada. El laboratorio de computación de la UACE, se encuentra equipado de tal manera que permite a los docentes exponer su cátedra y los estudiantes les permite poner en práctica lo aprendido, pero por percepción general se estima que este se necesita mejorar los procesos que se realizan en dicho lugar.

Para la presente investigación se manifiesta la importancia del control interno informático especialmente en entornos donde su uso es destinado a múltiples actividades y por diversos usuarios. Para lo cual el objetivo es: Proponer un Sistema de Control Interno Informático para salvaguardar los equipos tecnológicos en las instalaciones de los laboratorios de computación de la UACE de la UTMACH. Posteriormente se generará la metodología de control interno informático en donde se detallan todos los procesos para que el área informática trabaje de una manera correcta y alineada a las normas de seguridad actuales.

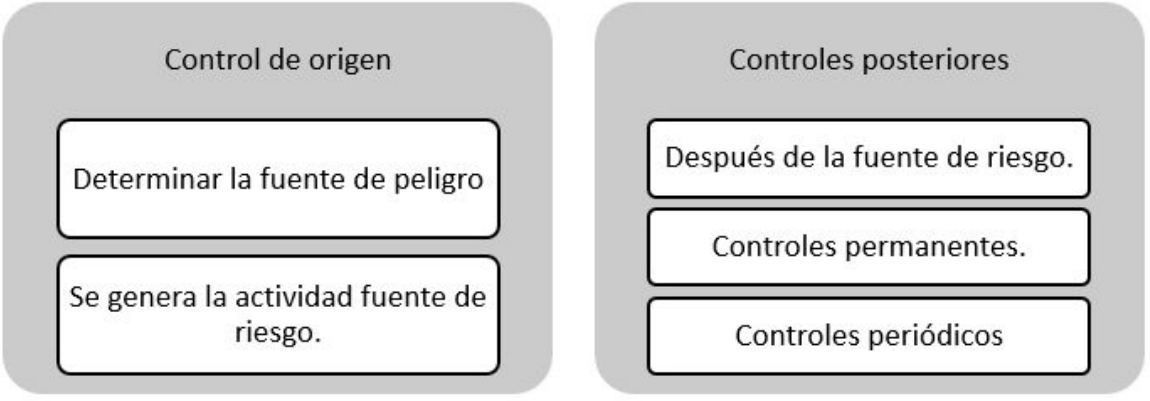
DESARROLLO

Control interno

Se conoce como control a aquella función con la que se espera asegurar el logro de los objetivos y los planes realizados con fundamento en la planificación (Dextre & Del Pozo, 2012). Dentro de las organizaciones, el control interno es de gran importancia, principalmente porque ofrece un enfoque de mejora continua, el cual también se dirige hacia todas las actividades que son parte de la organización y que son realizadas por la dirección y el resto de las personas que forman parte de la empresa.

Además el control interno también ayuda en el cumplimiento de los objetivos estratégicos de la organización, esto se debe a que permite la verificación y el esclarecimiento de los riesgos relacionados con las actividades que se llevan adelante en cada procesos, teniendo especial cuidado en resguardar los intereses de la empresa. De acuerdo a los niveles de riesgos, el control interno puede clasificarse en dos: controles de origen y controles posteriores.

Esquema 1. Clasificación del control



Fuente: (Calle, 2018).

Controles de origen.- Se encargan de que la fuente de peligro se encuentre dentro de los límites establecidos de tolerancia. La persona que se encuentra a cargo de este tipo de control, es quien genera la actividad catalogada como riesgosa.

Controles posteriores.- Se implementan luego de que la fuente de riesgo ha sido identificada, por lo tanto se deben diseñar estrategias para evitar perjuicios futuros, estos controles a su vez se sub-clasifican en: controles permanentes y periódicos:

- Controles permanentes.- Se llegan a implementar cuando lo fuente de riesgo posee altas probabilidades de exceder los límites de capacidad de la organización, esta es la razón por la que tienen el carácter de permanente.
- Controles periódicos.- Por el contrario si el riesgo, en sí no representa una amenaza, puede resultar suficiente el mantener controles periódicos, bajo este contexto la intensidad de las medidas adoptadas por la organización dependerá de las características que tenga el riesgo.

De esta manera un control adecuado permite identificar las vulnerabilidades y amenazas existentes, y una manera eficaz de lograrlo es a partir de los diagnósticos, que permitan conocer el estado de seguridad que presenta la empresa, poniendo clara atención en la normativa y en los procesos de análisis y evaluación de riesgos (Solarte, Enriquez, & Benavides, 2015). Otra manera de lograr los objetivos es el identificando los riesgos que se encuentran asociados a cada actividad, el cual debe sustentarse en el cuidado de los activos, lo interese comunes, la prevención de fraudes y errores y el cometimiento de riesgos innecesarios (Vargas, Arencibia, García, & Soto, 2017)

En base a lo expuesto, se puede afirmar que el control interno busca limitar los riesgos que pueden afectar a aquellas actividades que se realizan de forma normal dentro de las entidades, la forma de hacerlo es a partir de la investigación y el análisis de posibles riesgos y determinar la manera que, desde el control interno es factible disminuirlos, principalmente después de determinar las posibles vulnerabilidades (Gómez, Blanco, & Conde, 2013).

Desde el punto de vista del control interno, uno de los activos más importantes es la información, y su cuidado y protección es uno de los aspectos más relevantes, debido a este punto, para que el control interno tenga la característica de confiable, deberá asegurar que la información proviene de los datos informáticos es íntegra, fiable y además esta se encuentra resguardada.

Control Interno informático

En un mundo tan competitivo como el de hoy, resulta poco factible que una organización alcance el desarrollo, sin que disponga de un sistema de información que integre todos los niveles organizacionales, desde el directivo hasta el operativo, lo que le permite la toma de decisiones, y que estas sean las más acertadas y oportunas. Siendo de esta manera que los sistemas de información, al ser utilizados en función con la tecnología y la comunicación, se puede llevar de mejor manera la gestión de las organizaciones, convirtiendo también a la información en uno de sus activos más importantes (Comas, Nogueira, & Medina, 2014).

Con el uso de las tecnologías de la información y la comunicación nace el control informático, el cual tiene por objetivo asegurar que las medidas obtenidas por parte de los equipos informáticos implementados en la organización, sean utilizadas de forma adecuada y además éstas atiendan los requerimientos de la empresa. En respuesta a lo mencionado lo objetivos del control interno informático se enuncian a continuación:

- Protección a los activos de la información, entre los que se encuentran: los datos generados, el software y el hardware.
- El cumplimiento a las normas y leyes internas de la organización.
- Asegurar que los datos generados y custodiados sean íntegros y de alta precisión.
- Procesos fiables y además gran eficacia en el uso de los recursos.

De esta manera los sistemas de información se configuran como unidades integradoras entre el usuario y los equipos, cuyo objetivo es el de ofrecer información que ofrezca apoyo a las operaciones que realiza la organización, para ello hace uso de equipos de cómputo y software, diversos procedimientos, métodos de análisis, para la planeación, el control y como resultado, para la toma de decisiones (Solano, Riascos, & Aguilera, 2013).

En conclusión, la dependencia de la información y la generación de esta por medio de equipos informáticos, debe estar garantizada por el control interno, por lo que se hace necesario el uso de medios eficaces y eficientes que además garanticen la obtención de la calidad en los procesos y servicios y de esta manera se contribuye también a la protección y

conservación de la información evitando de esta manera el cometimiento de errores y posibles delitos.

Precisamente para evitar los posibles errores en el cumplimiento de las actividades rutinarias, las actividades que se realizan en los sistemas de control, pueden llegar a ser clasificados como: preventivos, detectivos y correctivos; también control de manual de usuario, control de cómputo y controles de tipo administrativo (Castañeda, 2014).

Esquema 2. Clasificación de las actividades de control

Control preventivo: Llegan también a ser conocidos como controles preliminares; estos son realizados antes de ejecutar las actividades de trabajo. Se aplica sobre la acción que causa el riesgo y principalmente sobre su agente generador, de esta manera se puede llegar a disminuir su probabilidad de ocurrencia, por muchos es considerado el mecanismo de control ideal (Orjuela, 2016).

Para su mejor ejecución es indispensable que los objetivos de la organización sean claros, para poder alcanzarlos, y que estos además se encuentren en concordancia con los recursos de los que dispone la organización. Desde este tipo de control se inspecciona las actividades durante el proceso de trabajo, por lo que a veces recibe el nombre de controles de dirección, los cuales monitorean las operaciones y las actividades, para de esta manera asegurar que las cosas se lleven a cabo de acuerdo a lo originalmente planeado.

Controles detectivos: Se refiere a la probabilidad de identificar el error o riesgo a partir de los controles generados por la organización (González, Myer, & Pachón, 2017). Su función se destina a encontrar eventos o irregularidades que no alcanzaron a ser advertidas y de la cuales no es posible conocer su resultado, por lo cual deben ser tomadas medidas a corregir el

hecho presentado. Estos sistemas sirven para la supervisión en los procesos realizados dentro de la organización y de esta manera también se verifica la eficacia que presentan los controles preventivos, por lo tanto también se los considera como una segunda barrera de seguridad. En base a lo mencionado se puede afirmar que sus funciones básicas corresponden a informar y registrar la ocurrencia de eventos no planificados, por lo que deben ser accionadas las alarmas de alerta y comunicación.

Controles correctivos: Se encargan de restablecer las actividades una vez que fue identificado un evento no planificado, por lo que se modifican las acciones que provocaron su ocurrencia. Estos controles son establecidos, una vez comprobado que los anteriores no operan, y en base a esto es posible mejorar los procesos y evitar posibles dificultades. Generalmente actúan en concordancia con los controles detectivos, en el replanteo de los procesos; entre sus características vale mencionar que son de tipo administrativo, por lo que para llevarse a cabo requieren de políticas y procedimientos.

Con respecto al control preventivo, su función aún es más importante, debido a que debe alertar ante un proceso de riesgo, o no planificado o no deseado y que este afecte directamente a lo que ocurre en la organización. El control detectivo este se encarga de avisar cuando un evento que no fue autorizado se encuentra registrado en el sistema, con el correctivo se llega a corregir la secuencia de errores o posibles hechos que generen singularidades dentro de la institución (Suárez, 2013).

Planes de contingencia para entornos informáticos.- El Plan de Contingencia llega a ser catalogado como una guía que contribuye a enfrentar cualquier suceso de riesgo. Estas medidas, de acuerdo al tipo de organización pueden ser: de controles físicos, de funciones, procedimientos y de programas, los cuales contribuyen a la protección íntegra de los datos, sino que también considera la seguridad física de los equipos y los ambientes donde estos se encuentren disponibles (Palacios & Quiroz, 2013). Desde este punto, la gestión de riesgos y el diseño e implementación de un sistema de control interno, permite la ejecución de acciones que resultan oportunas frente a diversos sucesos, especialmente cuando estas afectan el uso de los sistemas (López, Albanese, & Sánchez, 2014).

Planes de contingencia ante desastres tecnológicos.- Se refiere a la recuperación de desastres, donde resulta muy necesario controlar la situación presentada y llevar a cabo los procesos necesarios, sin que se vea afectada la información.

Caso práctico

La Universidad La Molina, se encuentran modernizando su Laboratorio de Computación y necesita implementar un Sistema de Control Interno Informático.

Pregunta a resolver:

¿Qué tipo de controles preventivos, detectivos y correctivos deberían implementarse en los laboratorios de la Universidad La Molina?

Antes de resolver el caso que compete, es indispensable hablar acerca de la protección de los recursos tecnológicos, entre los que se encuentran los equipos de computación, servidores, router, cables, etc., como apoyo a la información. Para llevar esto a cabo existen una serie de procesos que resultan determinantes para reducir los riesgos que puedan presentarse en el área física como en la información. También es importante hablar sobre la seguridad informática lo cual comprende la base de datos, la información, y el hardware, compuesto por las computadoras, servidores, impresoras, entre otros equipos.

El control interno informático será realizado en los laboratorios de la Unidad Académica de Ciencias Empresariales de la Universidad Técnica de Machala, para iniciar es indispensable establecer los objetivos del Control Interno Informático, los cuales se exponen a continuación:

- Determinar políticas y normas de seguridad en el uso de los equipos de computación.
- Analizar los estados en los que se encuentran los equipos de cómputo.
- Analizar el servicio utilizado, con el objetivo de verificar la confiabilidad en su uso

Etapa de evaluación del Sistema de Control Interno

Componentes	Preguntas	Si	No	Pod.	Calf.
Ambiente interno de control	¿El Laboratorio cuenta con alguna normativa para su uso?	x		10	0
	¿Se cuenta con otro lugar para el almacenamiento de los equipos?		x	10	10
	¿Se cuenta con un manual para el usuario, docente y personal?		x	10	0
Objetivos	¿Son conocidos los roles y responsabilidades de las personas que se encuentran encargadas del laboratorio?	x		10	5
	¿Se realizan periódicamente el mantenimiento de los equipos?	x		10	8
	¿Se han establecido objetivos para el laboratorio de computación?		x	10	0
	¿Alumnos y maestros respetan las normas del laboratorio de computación?	x		10	5
Identificación de eventos	¿El lugar donde se encuentra el laboratorio, es un área segura a las inundaciones, robo o cualquier otra situación que ponga en riesgo los equipos?		x	10	8
	¿Los laboratorios cuentan con salida de emergencia?		x	10	8

	¿Son comunicadas de forma oportuna las decisiones en cuanto al uso de los laboratorios?		x	10	8
Evaluación de riesgos	¿Se analizan los niveles de riesgo dentro del laboratorio?	x		10	2
	¿Se almacena junto con los equipos material que pueda resultar dañino?		x	10	
	¿La ubicación de los aires acondicionados es la adecuada?	x		10	7
	¿El cableado se encuentra correctamente instalado?	x		10	6
	¿Los interruptores de energía se encuentran debidamente protegidos?		x	10	4
	¿Se da mantenimiento a las instalaciones y al suministro de energía?		x	10	6
	¿Los laboratorios poseen extintores?	x		10	0
Actividades de control	¿Se implementan actividades de control a los riesgos?		x	10	0
	¿Se registra el acceso de los usuarios al laboratorio de computación?	x		10	8
	¿Se permite el acceso de información a los equipos de computación?		x	10	0
SUMAN				200	85

Calificación del riesgo

$$CR = \frac{85}{200} = 0{,}425$$

$$CR = 42{,}50\%$$

Nivel de confianza: 42,50%

Nivel de riesgo

$$NR = 100\% - 42{,}50\% = 57{,}5\%$$

Nivel de riesgo: 57,5%

Nivel de riesgo:	MODERADO ALTO
Nivel de confianza:	MODERADO BAJO

Controles

#	Riesgo	Preventivo	Detectivo	Correctivo
2	Normativa para el uso del laboratorio.	Aplicar políticas en cuanto al uso de los recursos de la institución .	Supervisión de las políticas para el uso adecuado de los recursos.	Mantenimiento de una política de seguimiento y control en cuanto al uso de los recursos.

3	Fallas en la comunicación entre el encargado y los usuarios.	Realizar la selección del talento humano en consideración a las competencias requeridas, además de monitoreo permanente a las competencias frente al desempeño demostrado.	Los resultados de la evaluación de competencias frente a su trabajo demostrada por el personal.	Capacitación, estimulación e incentivos o la reubicación y la reasignación de funciones.
4	Robo, daño o pérdida de los equipos informáticos.	Actualización de los inventarios.	Seguimiento y control de inventarios.	Solicitud de investigaciones administrativas ante presuntos robos o pérdida de inventario.
5	Mal uso de la web	Cada usuario debe conocer las políticas de uso de internet en los laboratorios.	Verificación de la existencia de programas dañinos a los equipos del laboratorio	Registro de las actividades realizadas en los equipos de cómputo y verificación del usuario responsable.

6	Interrupción de operaciones Por servicios básicos (interrupción de luz eléctrica, servicio de internet, entre otros).	Plan de contingencia para llevar a cabo las operaciones.	Pruebas periódicas de calidad y funcionamiento de los equipos y servicios informáticos.	Llevar a cabo el plan de contingencia.
7	Interrupción de las operaciones por conflictos laborales (ausencia del encargado)	Plan de contingencia (reemplazo)	Seguimiento al plan de contingencia.	Ajuste del Plan de Contingencia a las necesidades de la organización.

Para la Unidad Académica de Ciencias Empresariales de la UTMACH, una amenaza es todo objeto o sujeto o proceso capaz de atacar contra la seguridad de los equipos informáticos de los laboratorios de computación y estas se originan a partir de la existencia de fallas en el control interno del laboratorio.

Las amenazas a las que está expuesta el laboratorio de computación pueden ser intencionales y no intencionales. De esta manera las no intencionales se presentan al cometer una falla o un error que ponga en riesgo la integridad de los equipos, mientras que las intencionales son las que se llevan a cabo con el objeto de causar daño.

CONCLUSIONES

- El control informático tiene por objetivo fundamental el control de las actividades que se encuentran relacionadas con los sistemas de información automatizados, se realizan llevando a cabo las normas, estándares, procedimientos y disposiciones legales, establecidas de forma interna y externa.

- La identificación de los riesgos a los que se encuentran expuestos los equipos y las instalaciones del laboratorio de informática de la UACE contribuye al diseño de políticas y procedimientos que contribuyan a su buen uso.

- Es importante ejercer control y seguimiento de los procesos relacionados con el uso de los equipos del laboratorio de computación de la UACE.

- Promover el buen eso de los equipos e instalaciones de la UACE como mecanismo de control para el adecuado uso de los recursos.

BIBLIOGRAFÍA

Calle, J. (14 de Febrero de 2018). *Tipos de control interno de una empresa*. Obtenido de https://www.riesgoscero.com/blog/tipos-de-control-interno-de-una-empresa

Castañeda, L. (2014). Los sistemas de control interno en las Mipymes y su impacto en la efectividad empresarial. *En Contexto*(2), 1-258. Obtenido de http://ojs.tdea.edu.co/index.php/encontexto/article/view/139/124

Comas, R., Nogueira, D., & Medina, A. (2014). El control de gestión y los sistemas de información: propuesta de herramientas de apoyo. *Ingeniería Industrial*(2), 214-228.

Dextre, J., & Del Pozo, R. (2012). *¿Control de gestión o gestión de control?* Perú: Pontificia Universidad Católica del Perú.

Gómez, D., Blanco, B., & Conde, J. (2013). El Sistema de Control Interno para el Perfeccionamiento de la Gestión Empresarial en Cuba. *GECONTEC: Revista Internacional de Gestión del Conocimiento y la Tecnología, 1*(2), 53-65. Obtenido de https://search-proquest-com.ezproxybib.pucp.edu.pe/docview/1663910231/fulltextPDF/89A5A11065694C5FPQ/4?accountid=28391

González, J., Myer, R., & Pachón, W. (2017). La evaluación de los riesgos antrópicos en la seguridad corporativa: del Análisis Modal de Fallos y Efectos (AMFE) a un modelo de evaluación integral del riesgo. *Revista Científica General José María Córdova, 15*(19), 269-289. Obtenido de http://www.scielo.org.co/pdf/recig/v15n19/1900-6586-recig-15-19-00269.pdf

López, M., Albanese, D., & Sánchez, M. (2014). Gestión de riesgos para la adopción de la computación en nube en entidades financieras de la RepúblicaArgentina. *Contaduría y Administración,, 59*(3), 61-88. Obtenido de https://core.ac.uk/download/pdf/25651585.pdf

Orjuela, M. (2016). Elaboración de Sagrlaft para las empresas vigiladas por la superientendencia de las Sociedades, obligadas a reportar a la UIAF. *Apuntes Contables*(18), 9-29. Obtenido de https://revistas.uexternado.edu.co/index.php/contad/article/view/4663/5414

Palacios, R., & Quiroz, J. (2013). *PLAN DE CONTINGENCIA DE LOS EQUIPOS Y SISTEMAS INFORMÁTICOS EN EL GOBIERNO AUTÓNOMO*

DESCENTRALIZADO MUNICIPAL DEL CANTÓN JUNÍN. Manabí: Escuela Superior Politécnica Agropecuaria de Manabí.

Solano, O., Riascos, S., & Aguilera, A. (2013). Determinantes de los planes estratégicos de los sistemas de información en las Pymes colombianas: Caso Santiago de Cali - Colombia. *Entramado*(17), 26-37. Obtenido de http://www.scielo.org.co/pdf/entra/v9n1/v9n1a03.pdf

Solarte, F., Enriquez, E., & Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL – RTE, 28*(5), 492-507. Obtenido de http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321

Suárez, D. (2013). Una forma de interpretar la seguridad informática. *Innovación, Ingeniería y Desarrollo, 2*(2), 87-93. Obtenido de http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/IID/article/view/282/256

Vargas, Y., Arencibia, J., García, A., & Soto, D. (2017). Sistema Integral de Control Interno para el Vicedecanato de Administración y Servicios de la Facultad 3. *Serie Científica de la Universidad de las Ciencias Informáticas, 10*(2), 37-51.